Method for enabling later verification of already transmitted data.

Patent number: DE4234165
Publication date: 1994-03-03
Inventor: LOEHMANN EKKEHARD (DE); LUKAT JOERG (DE)
Applicant: DETECON GMBH (DE)
Classification:
- international: G09C5/00; H04L9/00; G06F12/16
- european: G09C5/00, H04L9/32B, G06F1/00N7R, G06F21/00N9C
Application number: DE19924234165 19921009
Priority number(s): DE19924234165 19921009

Also published as:
EP0597192 (A2)
EP0597192 (A3)
EP0597192 (B1)

Abstract not available for DE4234165
Abstract of correspondent: **EP0597192**

The method for enabling later verification of already transmitted data is based on the application of cryptographic methods for verifying the integrity and the authenticity of already transmitted personal data which have meantime been cleared (deleted). The transmitting entity transmits the data to a further entity, which confirms the unfalsified reception of the data. After the calculation of a cryptographic check sum with the use of a secret key, the transmitted data are cleared in the transmitting entity. In the event of renewed occurrence of the data in the transmitting entity, the cryptographic check sum and the secret key can be used to verify the integrity and authenticity of the data.

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Patentschrift**

(10) **DE 42 34 165 C1**

(51) Int. Cl.[5]:
G 09 C 5/00
H 04 L 9/00
G 06 F 12/16

(21) Aktenzeichen: P 42 34 165.5-31
(22) Anmeldetag: 9. 10. 92
(43) Offenlegungstag: —
(45) Veröffentlichungstag der Patenterteilung: 3. 3. 94

Innerhalb von 3 Monaten nach Veröffentlichung der Erteilung kann Einspruch erhoben werden

(73) Patentinhaber:
DETECON Deutsche Telepost Consulting GmbH, 53175 Bonn, DE

(72) Erfinder:
Lukat, Jörg, Dipl.-Inform., 5300 Bonn, DE;
Loehmann, Ekkehard, Dipl.-Math., 5330 Königswinter, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:
DE 37 05 736 C2

(54) Verfahren zur Ermöglichung der nachträglichen Überprüfung bereits übermittelter Daten

(57) Das Verfahren zur Ermöglichung der nachträglichen Überprüfung bereits übermittelter Daten beruht auf der Anwendung kryptographischer Verfahren zur Überprüfung der Integrität und der Authentizität bereits übermittelter, inzwischen gelöschter personenbezogener Daten. Die übermittelnde Instanz überträgt die Daten an eine weitere Instanz, die den unverfälschten Empfang der Daten bestätigt. Nach Berechnung einer kryptographischen Prüfsumme, unter Verwendung eines geheimen Schlüssels, werden die übermittelten Daten in der übermittelnden Instanz gelöscht. Bei erneuter Vorlage der Daten in der übermittelnden Instanz kann anhand der kryptographischen Prüfsumme und des geheimen Schlüssels die Integrität und Authentizität der Daten überprüft werden.

DE 42 34 165 C1

DE 42 34 165 C1

Beschreibung

Die Erfindung betrifft ein Verfahren zur Ermöglichung der nachträglichen Überprüfung bereits übermittelter Daten ohne die Erforderlichkeit, diese Daten für eine spätere Überprüfung in der übermittelnden Instanz zu speichern, wobei die Überprüfung der Integrität und der Authentizität bereits übermittelter, inzwischen gelöschter personenbezogener Daten auf der Anwendung kryptographischer Verfahren beruht. Kryptographische Verfahren werden bereits in Datenverarbeitungsanlagen zur Sicherung von Programmen und zur Integritätskontrolle gesicherter Programme eingesetzt.

Aus der DE-PS 37 05 736 ist ein solches Verfahren zur Sicherung der in dem Systemspeicher einer Datenverarbeitungsanlage enthaltenen Programme gegen Änderung und zur Integritätskontrolle gesicherter Programme bekannt. Bei diesem Verfahren werden die Programme zur Bildung einer Prüfziffer nach einem symmetrischen kryptographischen Algorithmus unter Verwendung eines lesegeschützt gespeicherten geheimen Schlüssels verschlüsselt. Die so gebildete Prüfziffer wird im Systemspeicher gespeichert. Zur Integritätskontrolle der Programme findet ein nochmaliges derartiges Verschlüsseln der Programme sowie ein Vergleich der so erhaltenen Prüfziffer mit der zugehörigen gespeicherten Prüfziffer statt.

Es ist bekannt, daß zur Prüfung eventueller Beschwerden hinsichtlich der Korrektheit von übermittelten Daten eine Kopie dieser übermittelten Daten für eine bestimmte Dauer von der übermittelnden Instanz gespeichert wird.

Der Nachteil dieses Verfahrens liegt in dem enormen Kostenaufwand, der für die Speicherung und Erhaltung der Daten betrieben werden muß. Zum einen fallen Kosten für die Speicherung (Lager, Geräte usw.) während des Zeitraum der Datenerhaltung an, zum anderen stellen Maßnahmen, die zur Sicherung der Daten gegen Verlust und Mißbrauch getroffen werden müssen, einen erheblichen Kostenfaktor dar.

Der Erfindung liegt deshalb die Aufgabe zugrunde, ein Verfahren aufzuzeigen, das es ermöglicht, eine Überprüfung der Daten auf Integrität und Authentizität zu gewährleisten, ohne daß die übermittelten Daten von der übermittelnden Instanz für die Dauer der Einspruchsfrist gespeichert werden müssen.

Die Vorteile des erfindungsgemäßen Verfahrens liegen in der Senkung der Kosten. Die Kosten für die Maßnahmen zur Einhaltung der datenschutzrechtlichen Bestimmungen entfallen. Außerdem wird der Umfang der Daten, die gespeichert werden müssen, im allgemeinen stark reduziert, wodurch die Datenhaltungskosten gesenkt werden.

Die Aufgabe wird durch die im kennzeichnenden Teil des Patentanspruchs 1 angegebenen Merkmale gelöst. Das erfindungsgemäße Verfahren beruht auf der Anwendung kryptographischer Verfahren zur Überprüfung der Integrität und der Authentizität bereits übermittelter, inzwischen gelöschter personenbezogener Daten. An diesem Verfahren sind mindestens zwei Instanzen beteiligt. Auf der übermittelnden Seite sitzt die Instanz A, die die Daten an eine zweite Instanz B übermittelt. Bevor die Übermittlung und das darauffolgende Löschen der Daten durch die Instanz A stattfindet, berechnet diese eine kryptographische Prüfsumme der Daten. Das Ergebnis der Berechnung der kryptographischen Prüfsumme hängt sowohl von den Daten selbst als auch von einem geheimen Schlüssel Ks ab. Zur Berechnung der kryptographischen Prüfsumme wird eine Einwegfunktion angewendet, was bedeutet, daß aus der kryptographischen Prüfsumme und dem geheimen Schlüssel Ks die Daten nicht wiedergewonnen werden können. Trotzdem kann bei erneuter Vorlage der Daten anhand der kryptographischen Prüfsumme und des geheimen Schlüssels Ks die Integrität und Authentizität der Daten überprüft werden.

Ein Beispiel des erfindungsgemäßen Verfahrens wird im folgenden anhand der Fig. 1 näher erläutert. Die zu übermittelnden Daten, sind bei der Instanz A (11) gespeichert. Bevor eine Übermittlung der betreffenden Daten an die Instanz B (12) erfolgt, berechnet die Instanz A die kryptographische Prüfsumme KP (13) der Daten (14) in Abhängigkeit von dem geheimen Schlüssel Ks (15). Danach speichert (16) die Instanz A die Daten, die kryptographische Prüfsumme KP und den geheimen Schlüssel Ks unter einer Zugriffsadresse ID (17) ab. Bei Bedarf übermittelt die Instanz A an die Instanz B die gewünschten Daten sowie die Zugriffsadresse ID mit dem Hinweis (18), daß die Daten gelöscht werden, sobald die Instanz B den unverfälschten Empfang bestätigt (19), und daß die Daten von der Instanz A nicht rekonstruiert werden können, sondern daß nur bei Vorlage der Zugriffsadresse ID und der Daten die Integrität und die Authentizität der Daten geprüft werden kann. Nachdem die Instanz B der Instanz A den unverfälschten Empfang der Daten bestätigt hat, löscht die Instanz A die unter der Zugriffsadresse ID gespeicherten Daten wobei die kryptographische Prüfsumme KP und der geheime Schlüssel Ks weiterhin bei der Instanz A gespeichert bleiben. Kommt es nun gegenüber der Instanz B zu einer Beschwerde (20) über die Korrektheit der Daten, legt die Instanz B der Instanz A die strittigen Daten und die zugehörige Zugriffsadresse ID vor. Instanz A berechnet unter Berücksichtigung des unter der Zugriffsadresse ID gespeicherten geheimen Schlüssels Ks die kryptographische Prüfsumme KP' (21) der vorgelegten Daten. Stimmt die kryptographische Prüfsumme KP' der vorgelegten Daten mit der bei der Instanz A unter der Zugriffsadresse ID gespeicherten kryptographischen Prüfsumme KP bitgenau überein, so werden die vorgelegten Daten als integer und authentisch anerkannt. Instanz A kann jetzt wie gewohnt die Beschwerde weiterverfolgen.

Eine Variante zu dem eben beschriebenen Verfahren wird in Fig. 2 erläutert. Wie bei dem ersten Verfahren berechnet die Instanz A (11) die kryptographische Prüfsumme KP (13) der Daten (14) in Abhängigkeit von dem geheimen Schlüssel Ks (15) und speichert die Daten, die kryptographische Prüfsumme KP und den geheimen Schlüssel Ks unter einer Zugriffsadresse ID (17) ab. Im Gegensatz zu dem oben beschriebenen Verfahren übermittelt die Instanz A an die Instanz B die Daten, die kryptographische Prüfsumme KP und die Zugriffsadresse ID aber diesmal mit dem Hinweis (18) das die Daten und die kryptographische Prüfsumme KP gelöscht werden, sobald die Instanz B den unverfälschten Empfang bestätigt, und daß die Daten von der Instanz A nicht rekonstruiert werden können, sondern daß nur bei Vorlage der Zugriffsadresse ID, der Daten und der kryptographischen Prüfsumme KP die Integrität und die Authentizität der Daten bestätigt werden kann. Nachdem die Instanz B der Instanz A den unverfälschten Empfang der Daten und der kryptographischen Prüfsumme KP bestätigt hat (19), löscht die Instanz A sowohl die unter der Zugriffsadresse ID gespeicherten Daten als auch die kryptographische Prüfsumme KP.

Nur der geheime Schlüssel Ks bleibt weiterhin bei der Instanz A gespeichert. Kommt es nun zum Beschwerdefall (20), legt Instanz B der Instanz A die strittigen Daten, die zugehörige kryptographische Prüfsumme KP und die zugehörige Zugriffsadresse ID vor. Instanz A berechnet nun unter Berücksichtigung des unter der Zugriffsadresse ID gespeicherten geheimen Schlüssels Ks die kryptographische Prüfsumme KP' (21) der vorgelegten Daten. Stimmt die berechnete kryptographische Prüfsumme KP' der vorgelegten Daten mit der von Instanz B vorgelegten kryptographischen Prüfsumme KP bitgenau überein, so werden die vorgelegten Daten als integer und authentisch anerkannt. Instanz A kann jetzt wie gewohnt die Beschwerde weiterverfolgen.

Für die Berechnung der kryptographischen Prüfsumme können verschiedene kryptographische Verfahren herangezogen werden. Die kryptographische Prüfsumme kann z. B. durch die Berechnung eines MACs (Massage Authentication Code) gebildet werden, wobei in diesem Fall der für die Erzeugung des MACs benötigte geheime Schlüssel bei der Instanz A und nur bei ihr gespeichert wird. Dies ist der Unterschied zur Verwendung des MACs im herkömmlichen Sinn, bei der ja die Daten (Message) zwischen zwei Kommunikationspartnern ausgetauscht werden, die beide über den geheimen Schlüssel verfügen müssen. Dadurch ist auch kein Schlüsselmanagement erforderlich, da die erzeugende und die überprüfende Instanz ein und dieselbe Instanz ist.

Eine zweite Möglichkeit besteht darin, die kryptographische Prüfsumme durch die Berechnung einer digitalen Unterschrift zu bilden. Wenn es für die weitere Beschwerdebearbeitung erforderlich ist einem Dritten zu beweisen, daß die strittigen Daten so übermittelt worden sind oder eben nicht, so ist es notwendig die kryptographische Prüfsumme mittels eines Signaturverfahrens mit asymmetrischen Schlüsseln zu berechnen. Hierzu muß der Beschwerdeführer und der urteilende Dritte natürlich Kenntnis von dem öffentlichen Schlüssel des Senders haben.

Ein Ausführungsbeispiel erläutert die Erfindung. In den D-Netzen werden Mobilfunkdienste den Teilnehmern durch Dienstanbieter angeboten, die eigene Kundenverträge mit Teilnehmern unterhalten und eigene Rechnungen über die in Anspruch genommenen Dienste schreiben.

Um dies zu ermöglichen, ist es erforderlich, daß der Netzbetreiber die Verbindungsdaten der Kunden seiner Dienstanbieter an den jeweiligen Dienstanbieter zum Zweck der Entgeltermittlung und Entgeltabrechnung seiner Kunden übermittelt. Durch das deutsche Recht wird dem Kunden die Wahl gegeben, ob seine Verbindungsdaten nach Versendung der Entgeltrechnung vollständig gelöscht, unter Verkürzung der Zielrufnummer um die letzten drei Ziffern für 80 Tage gespeichert oder vollständig für 80 Tage gespeichert werden sollen. Diese Vorschrift betrifft insbesondere die Verbindungsdaten, die der Netzbetreiber und der Dienstanbieter für seine eigenen Kunden zum Zwecke der Beschwerdebearbeitung speichert, aber auch die Verbindungsdaten, die für die Abrechnung bzw. Beschwerdebearbeitung des Netzbetreibers mit dem Dienstanbieter bzw. durch den Netzbetreiber erforderlich sind. Das heißt, der Netzbetreiber muß auch die Verbindungsdaten der Kunden seiner Dienstanbieter entsprechend deren Wahl selektiv löschen. Dieses rechenintensive selektive Löschen der Verbindungsdaten kann durch Anwendung des oben beschriebenen Verfahrens in der Weise vermieden werden, daß der Netzbetreiber zu jedem Verbindungsdatensatz eines Kunden seines Dienstanbieters die kryptographische Prüfsumme berechnet.

Unter der Voraussetzung, daß die letzten drei Ziffern der Zielrufnummer des Verbindungsdatensatzes für die Abrechnung des Netzbetreibers mit dem Dienstanbieter unerheblich ist, ist es ausreichend, eine kryptographische Prüfsumme 1 über den Verbindungsdatensatz mit Ausnahme der letzten drei Ziffern der Zielrufnummer zu bilden; andernfalls ist es notwendig, eine weitere kryptographische Prüfsumme 2 über den gesamten Verbindungsdatensatz zu bilden. Der Netzbetreiber übermittelt wie gewohnt die Verbindungsdatensätze an den Dienstanbieter, speichert nach Bestätigung des unverfälschten Empfangs unter der Zugriffsadresse ID den geheimen Schlüssel Ks und die kryptographische Prüfsumme 1 (ggf. die kryptographische Prüfsumme 2) für die Dauer der Beschwerdefrist und löscht den eigentlichen Verbindungsdatensatz. Da der Netzbetreiber die datenschutzrechtlichen sensiblen Verbindungsdaten insgesamt gelöscht hat, kann er auf das selektive Löschen nach Wahl des Kunden des Dienstanbieters verzichten. Beschwert sich ein Kunde eines Dienstanbieters über seine Fernmelderechnung, so kann der Netzbetreiber die Prüfung der Integrität und Authentizität den dem Dienstanbieter verbliebenen und zur Beschwerdeverfolgung an ihn zurückübermittelten strittigen Daten, wie oben beschrieben, anhand der gespeicherten Werte kryptographische Prüfsumme 1 bzw. kryptographische Prüfsumme 2 durchführen und wie gewohnt verfolgen.

Das Verfahren läßt sich in den beiden Varianten auch auf nicht elektronische Dokumente anwenden. In diesem Fall werden der Instanz B die Daten und gegebenenfalls die kryptographische Prüfsumme zum Beispiel in Form eines Aktenzeichens in einem Papierbrief übermittelt. Im Beschwerdefall wird der strittige Datensatz und gegebenenfalls die kryptographische Prüfsumme aus den Angaben der Instanz B und dem Aktenzeichen wiedergewonnen, und die Überprüfung kann wieder auf elektronischem Weg, wie bisher beschrieben, erfolgen.

Patentansprüche

1. Verfahren zur Ermöglichung der nachträglichen Überprüfung bereits übermittelter Daten ohne die Erforderlichkeit, diese Daten für eine spätere Überprüfung in der übermittelnden Instanz zu speichern, **dadurch gekennzeichnet**, daß die übermittelnde Instanz vor der ersten Übermittlung eine kryptographische Prüfsumme der Daten, unter Anwendung der Daten und eines geheimen Schlüssels, berechnet und diese kryptographische Prüfsumme unter einer Zugriffsadresse abspeichert, wobei nach der Übermittlung mindestens der Daten und der Zugriffsadresse an mindestens eine weitere Instanz die übermittelten Daten in der übermittelnden Instanz nach Bestätigung des unverfälschten Empfangs der übermittelten Daten durch die weitere Instanz unrekonstruierbar gelöscht werden, wobei durch Speicherung zumindest des Schlüssels und der Zugriffsadresse in der übermittelnden Instanz, durch eine Rückübermittlung mindestens der Daten und der Zugriffsadresse durch die weitere Instanz an die übermittelnde Instanz eine zweite kryptographische Prüfsumme unter Anwendung des geheimen Schlüssels erneut von der übermittelnden Instanz berechnet wird, wobei dann beim Vergleich der zweiten kryptographischen Prüfsum-

me mit der zuerst errechneten kryptographischen Prüfsumme und Übereinstimmung der beiden berechneten kryptographischen Prüfsummen die Authentizität und Integrität der Daten festgestellt wird.

2. Verfahren gemäß Patentanspruch 1, dadurch gekennzeichnet, daß die kryptographischen Prüfsumme mittels einer Einwegfunktion berechnet wird.

3. Verfahren gemäß einem der obigen Patentansprüche, dadurch gekennzeichnet, daß die Einwegfunktion anhand eines MACs (Message Authentication Code) gebildet wird.

4. Verfahren gemäß einem der obigen Ansprüche, dadurch gekennzeichnet, daß der für die Erzeugung des MACs benötigte geheime Schlüssel in der übermittelnden Instanz gespeichert wird und nur bei dieser.

5. Verfahren gemäß einem der obigen Patentansprüche dadurch gekennzeichnet, daß nur die übermittelnde Instanz den geheimen Schlüssel kennt und dadurch gleichzeitig die erzeugende Instanz der kryptographischen Prüfsumme ist, als auch die überprüfende Instanz der Daten auf Integrität und Authentizität darstellt.

6. Verfahren gemäß einem der obigen Patentansprüche, dadurch gekennzeichnet, daß die kryptographische Prüfsumme durch die Berechnung einer digitalen Unterschrift gebildet wird.

7. Verfahren gemäß einem der obigen Patentansprüche, dadurch gekennzeichnet, daß die Übermittlung der Daten auf elektronische und nicht elektronische Weise erfolgen kann.

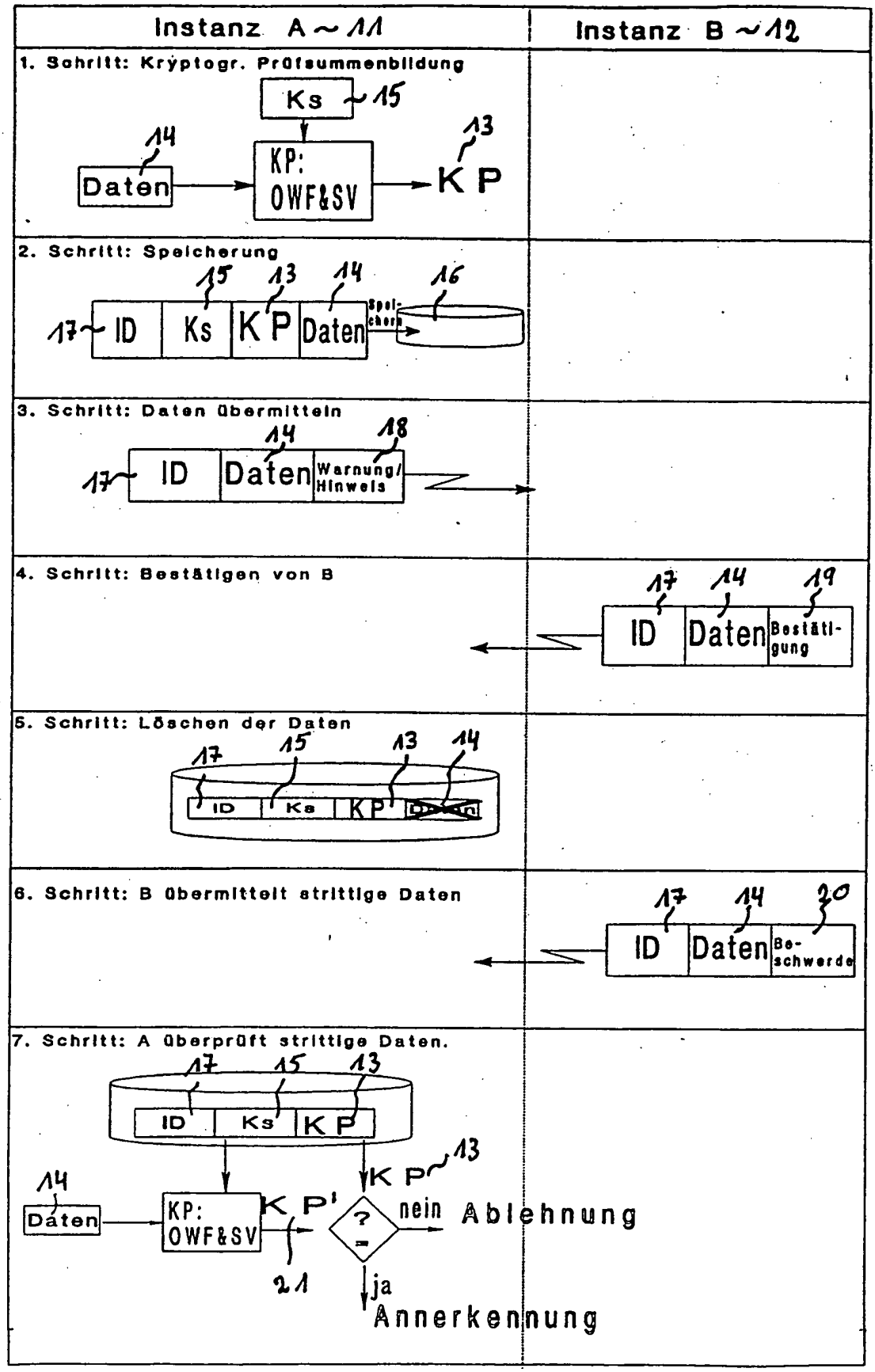
8. Verfahren gemäß einem der obigen Patentansprüche, dadurch gekennzeichnet, daß die Daten und die kryptographische Prüfsumme nach der Übermittlung der Daten, der kryptographischen Prüfsumme und der Zugriffsadresse durch die übermittelnde Instanz in der übermittelnden Instanz gelöscht werden.

9. Verfahren gemäß einem der obigen Ansprüche dadurch gekennzeichnet, daß für die Berechnung der kryptographischen Prüfsumme jedem neuen Datensatz ein neuer geheimer Schlüssel zugeordnet werden kann.

Hierzu 2 Seite(n) Zeichnungen

Nummer: DE 42 34 165 C1
Int. Cl.[5]: G 09 C 5/00
Veröffentlichungstag: 3. März 1994

Fig. 1



Nummer: DE 42 34 165 C1
Int. Cl.5: G 09 C 5/00
Veröffentlichungstag: 3. März 1994

Fig. 2